Health Information Compliance Alert

Compliance: Learn 3 Big Lessons From The HITECH Annual Reports

How to avoid the top 4 causes of HIPAA breaches

The **HHS Office for Civil Rights** (OCR) recently released some surprising data in two in-depth reports on HIPAA compliance and breaches. Luckily, the reports also contained a few gems of advice to healthcare providers that will help you prevent a HIPAA catastrophe.

On June 11, OCR issued two reports to Congress mandated by the Health Information Technology for Economic and Clinical Health (HITECH) Act: "Breaches of Unsecured Protected Health Information" and "HIPAA Privacy, Security, and Breach Notification Rule Compliance." The reports cover calendar years 2011 and 2012.

What the Reports Had to Say

The breach notification report provides an overview of the breach notification requirements, while the report on the HIPAA rules summarizes complaints that HHS has received of alleged violations of HITECH and the HIPAA Privacy and Security Rules, according to OCR.

During 2011 and 2012, the reports state that HHS entered into seven resolution agreements/corrective action plans totaling more than $8 million in settlements, reported Milwaukee, WI-based attorney **Meghan O'Connor** in a June 12 blog posting for the law firm v**on Briesen & Roper, S.C**. These settlements resulted from breaches reported to HHS, which spurred investigations. OCR received 236 reports in 2011 and 222 reports in 2012 of breaches involving 500 or more individuals.

"The compliance report reviews HHS compliance and enforcement activities, as well as complaints received by HHS with respect to the HIPAA Privacy, Security, and Breach Notification Rules," O'Connor said. From 2003 to 2012, OCR investigated 27,466 complaints and resolved 18,559 of these cases by requiring corrective actions and/or providing technical assistance.

Avoid the Top 4 Causes of HIPAA Breaches

O'Connor pointed out that, according to the breach report, the primary reported causes of larger breaches included:

- Theft;
- Unauthorized access, use, or disclosure;
- Improper disposal; and
- Hacking/IT incident.

"Based on the types of breach reports submitted, HHS advises that entities subject to HIPAA should ensure completing of risk evaluations, secure portable electronic devices, provide for proper disposal of PHI, implement physical access controls, and provide trainings to members of the workforce," stated a June 20 blog posting by health law attorney **Leah Roffman** for the law firm **Cooley LLP**. "These are important steps to take to limit the likelihood of a breach."

And although these reports may seem simply like jumbles of depressing statistics, you can actually learn quite a bit from them. Here are three key lessons you can glean from these reports:

1. Ratchet Up Your Theft-Prevention Efforts

Theft didn't merely rank number one on the list of breach causes, it blew all other causes out of the water. Theft accounted for half of the breaches in both years (50 percent in 2011 and 53 percent in 2012), according to Roffman.

"The statistics in both reports clearly show that the most breaches still come from 'older' sources of PHI, such as paper records, desktop computers, and network servers," noted attorneys **Stephanie Willis** and **Dianne Bourque** in an analysis for the law firm **Mintz Levin Cohn Ferris Glovsky and Popeo PC**, which was published in The National Law Review on June 20.

"In addition to updating and monitoring security protocols for older PHI sources, covered entities should address security problems with newer storage media," according to Willis and Bourque.

And specifically, the breach report also shows a large increase in the number of breaches involving laptops, said Willis and Bourque. "Because theft was the primary cause of breaches in 2009 to 2012, ensuring that laptops and other portable devices are secured in accordance with standards acceptable under HIPAA will become even more important as organizations adopt more 'bring your own device' policies to ensure the mobility and convenience of health care delivery."

2. Keep a Close Eye on Your BAs

Although BAs accounted for only 26 percent of the breaches in the reporting period, these breaches affected 59.3 percent of the total individuals affected by all the breaches reported. And the large number of affected individuals in breaches involving BAs likely reflects the reality that BAs may house PHI for multiple CEs, Willis and Bourque pointed out.

Action point: "Based on these statistics, health care organizations must impose standards for using BAs and subcontractors," Willis and Bourque urged. You must also ensure that your BAs and subcontractors understand their obligations under the HIPAA Privacy and Security Rules.

3. Beware of the Cumulative Effects of Small Breaches

Although small breaches those involving fewer than 500 individuals may seem like a far cry from mega breaches affecting millions of people, they can still seriously hurt your organization.

Reason: "The problem with small breaches for organizations is that they can occur more frequently than large ones," warned Willis and Bourque. "The occurrence of repeated small breaches can be indicative of a systemic compliance problem, and may suggest to a regulator that the organization has not taken steps to identify and remedy the problem."

That's why it's crucial for your organization to determine its breach risk profile, and identify and correct any compliance gaps, Willis and Bourque stressed. "All covered entities should ensure that they account for the likelihood of small breaches as much as they do for large breaches when doing their security risk assessments." (For help with your risk assessment, check out the **HHS Office of the National Coordinator's** Security Risk Assessment Tool for small and medium-sized health care providers at www.healthit.gov/security-risk-assessment.)

Links: To access the breach notifications report, go to www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachreptmain.html. The report on the HIPAA rules is available at www.hhs.gov/ocr/privacy/hipaa/enforcement/compliancereptmain.html.